(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2001－242785
（P2001－242785A）
(43)公開日　平成13年９月７日(2001.9.7)

(51)Int.Cl.[7]	識別記号	ＦＩ	テーマコード（参考）
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｂ
			６４０Ｚ
	６６０		６６０Ａ
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｂ
			３２０Ｆ

審査請求　未請求　請求項の数３　ＯＬ　公開請求　（全　８　頁）

(21)出願番号　特願2001－123147(P2001－123147)

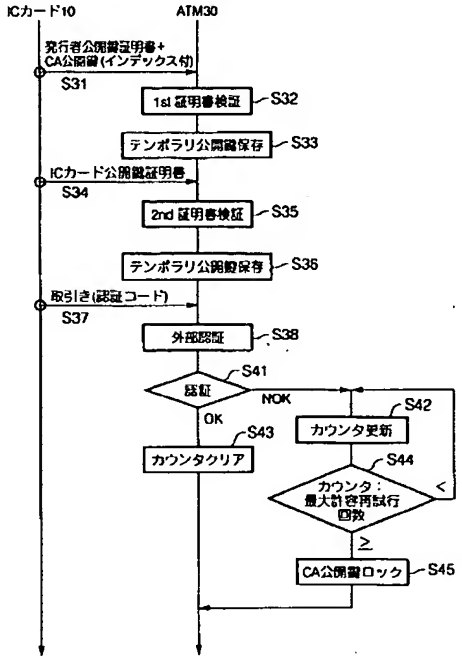
(22)出願日　平成13年４月20日(2001.4.20)

(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号
(71)出願人　501161756
社団法人東京銀行協会
東京都千代田区丸ノ内一丁目３番１号
(71)出願人　399035766
エヌ・ティ・ティ・コミュニケーションズ株式会社
東京都千代田区内幸町一丁目１番６号
(74)代理人　100064908
弁理士　志賀　正武　（外２名）

最終頁に続く

(54)【発明の名称】　ディジタル署名システム

(57)【要約】
【課題】　秘密鍵を複数持つディジタル署名システムにおける公開鍵の特定と、複数階層の証明書検証処理の効率化をはかる。
【解決手段】　どの秘密鍵を利用した証明書かを特定するためのインデックスを付与してノードに送信し、当該ノードでインデックスに関連付けられた公開鍵を特定して検証を行なう。また、あるノードで証明書が検証された公開鍵をＩＣカード１０の一時記憶領域に格納し、この公開鍵を指定して次のノードにおける証明書の検証を行ない、更に検証された公開鍵を用いて外部認証コードを検証し取引を行なう。



【特許請求の範囲】
【請求項１】　秘密鍵を複数持つディジタル署名システムにおいて、
どの秘密鍵を利用した証明書かを特定するためのインデックスを付与してノードに送信し、当該ノードで前記インデックスに関連付けられた公開鍵を特定して検証を行なうことを特徴とするディジタル署名システム。
【請求項２】　少なくとも２つのノードで証明書を持ち、前記各証明書を検証した後、当該検証された公開鍵を用いて外部認証コードを検証しカード取引を行なうディジタル署名システムにおいて、
前記あるノードにおいて前記証明書が検証された公開鍵をＩＣカードの一時記憶領域に格納し、前記一時記憶領域に格納された公開鍵を指定して次のノードにおける証明書の検証を行ない、前記検証された公開鍵を用いて外部認証コードを検証し、カード取引を行なうことを特徴とするディジタル署名システム。
【請求項３】　前記外部認証コードの検証に失敗した場合、最初に利用した公開鍵に付加されたカウンタに設定される最大許容再試行回数を超えたときに前記公開鍵の利用を禁止することを特徴とする請求項２に記載のディジタル署名システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、複数世代の公開鍵管理と複数階層の証明書検証を実現するディジタル署名システムに関する。
【０００２】
【従来の技術】ディジタル署名は、公開鍵暗号化方式や秘密鍵暗号化方式と組み合わせて複合的なシステムの中で利用される。公開鍵暗号化方式を利用することから、実用するためには認証局（ＣＡ）が運営される。
【０００３】ディジタル署名を金融機関に応用した場合の認証局体系および証明書管理について図６にその概要が示されている。図６において、符号６１は金融機関、符号６２は認証局、符号６３はＡＴＭ等の金融端末、符号６４はＩＣカードである。まず、認証局６２（以下、単にＣＡ６２と称する）は、金融機関６１の申請に基づき証明書の発行を行うスキーム管理局である。カード発行者である金融機関６１は、ＣＡ６２に自身の公開鍵を登録し、当該鍵に対する証明書を発行してもらう。また、金融機関６１は、自らが発行する各ＩＣカード６４に対する公開鍵、秘密鍵のペアを作成し、自身の秘密鍵によって証明書を生成する。ＡＴＭ等各金融端末６３においては、個々の端末に対する公開鍵、秘密鍵のペアを作成し、ＣＡ６２により生成された証明書をＡＴＭ等金融端末６３に格納する。
【０００４】ところで、上記した公開鍵暗号化方式では、安全性の根拠の一つを、解読の際における計算量の多さにおいている。従って、同一の公開鍵や秘密鍵を長期間使用し続けることは安全性の低下につながるため、証明書の発行者は、それに付与するディジタル署名の生成用秘密鍵を定期的に更新しなければならない。その際、現在のサービスを中断することなく、かつＩＣカード６４とＡＴＭ等金融端末６３との間の認証に必要なデータの整合性を確保した管理に基づく必要がある。
【０００５】
【発明が解決しようとする課題】これに対し、従来のＩＣカード６４におけるＡＴＭ等金融端末６３を利用した証明書検証によれば、ある領域に格納された公開鍵を用いて検証が行なわれるため、ＣＡ６２の秘密鍵の更新に同期して更新される公開鍵を入手する必要があり、上記した定期的な更新により２種類以上の証明書が出回る可能性があって、ＩＣカード６４ではその整合性を加味した検証を行なうことはできなかった。
【０００６】また、従来、ＩＣカード６４内に保持する公開鍵を用いて証明書を検証するのに、その証明書を検証するコマンドとは別に、検証され、取り出された公開鍵を用いて外部認証コードの検証を行なうコマンドの実行を要していた。従って、金融システムのように、証明書の検証が、ＣＡ６２－外部ノード発行者（金融機関６１）－外部ノード（ＩＣカード６４）といった複数階層を持つものにおいては、それぞれの階層における証明書の検証で得られる公開鍵が次の階層における証明書の検証に反映されず、従って、繰り返し動作により、効率的な証明書の検証、公開鍵の抽出ができなかった。特に、検証に失敗した場合等においては、証明書のデータ量が比較的大きいため、少ない記憶容量しか持たないＩＣカードにあっては致命的な問題となる。
【０００７】本発明は上記事情に鑑みてなされたものであり、ＩＣカードにＣＡ公開鍵とその世代を示すインデックスとを組み合わせて複数格納し、ＩＣカードで外部ノードの公開鍵証明書を検証する場合、公開鍵証明書と共にその証明書を付与したＣＡのインデックスと共にＩＣカードに送信し、ＩＣカード内で格納されたデータと送信されたデータを照合し関連付けられたＣＡ公開鍵を用いて検証することにより、セキュリティを高め、かつ、信頼性及び処理速度の向上を図ったディジタル署名システムを提供することを目的とする。
【０００８】また、ＩＣカードの公開鍵証明書を検証するコマンドに、一時的に格納された鍵を用いて検証するインタフェースを付加することにより、ＣＡ公開鍵を用い証明書が検証された公開鍵を一時記憶領域に格納し、その公開鍵を指定して次階層の証明書の検証を行ない、外部認証を行なうことができ、複数階層の証明書検証を効率的に、かつ、記憶容量の節約と汎用性の向上を図ったディジタル署名システムを提供することも目的とする。
【０００９】
【課題を解決するための手段】上記した課題を解決する

ために本発明は、秘密鍵が複数存在するディジタル署名システムにおいて、どの秘密鍵を利用した証明書かを特定するためのインデックスを付与してノードに送信し、当該ノードで前記インデックスに関連付けられた公開鍵を特定して検証を行なうことを特徴とする。

【００１０】上記した課題を解決するために本発明は、少なくとも２つのノードで証明書を持ち、前記各証明書を検証した後、当該検証された公開鍵を用いて外部認証コードを検証しカード取引を行なうディジタル署名システムにおいて、前記あるノードにおいて前記証明書が検証された公開鍵をＩＣカードの一時記憶領域に格納し、前記一時記憶領域に格納された公開鍵を指定して次のノードにおける証明書の検証を行ない、前記検証された公開鍵を用いて外部認証コードを検証しカード取引を行なうことを特徴とする。

【００１１】また、本発明のディジタル署名システムにおいて、前記外部認証コードの検証に失敗した場合、最初に利用した公開鍵に付加されたカウンタに設定される最大許容再試行回数を超えたときに前記公開鍵の利用を禁止することを特徴とする。

【００１２】上記構成において、ＩＣカード内にＣＡ公開鍵とそのＣＡのインデックスを組み合わせて複数格納し、ＩＣカードで外部ノードの公開鍵証明書を検証するとき、公開鍵証明書と共にその証明書を付与したＣＡのインデックスと共にＩＣカード内に送信し、ＩＣカードでは、その格納されたＣＡのインデックスと送信されるＣＡのインデックスとを照合し、関連付けられたＣＡ公開鍵で検証することで、複数種類の秘密鍵による証明書が出回ってもＩＣカードでの検証を可能とし、セキュリティを維持しながら信頼性及び処理速度の向上が図られる。また、上記構成において、ＣＡ公開鍵を用いて証明書が検証された公開鍵はテンポラリ公開鍵としてＩＣカード内に保存され、ＩＣカードの証明書を検証するコマンドを用いてそのテンポラリ公開鍵を指定し、当該テンポラリ公開鍵を用いて証明書を検証し、証明書が検証された公開鍵はテンポラリ公開鍵として保存される。そして、外部認証時、そのテンポラリ公開鍵を用いた検証を行なうことで、ＩＣカードの記憶容量の節約ができ、また、１つのコマンドで証明書の検証ならびに公開鍵の抽出を実現できるため、検証のための処理速度の改善がはかれる。

【００１３】

【発明の実施の形態】図１は、本発明が採用されるＩＣカードの内部構成を示すブロック図である。ＩＣカード１０は、ＣＰＵ１１を制御中枢とし、プログラムメモリ１２、データメモリ１３、入出力インタフェース回路１４が内部バス１５に共通接続されて成る。入出力インタフェース回路１４は、ＡＴＭ端末等外部から到来するコマンドもしくはデータを受信して内部バス１５を介してＣＰＵ１１に伝える他、ＣＰＵ１１によって処理されたデータを外部に供給する双方向の回路である。

【００１４】ＣＰＵ１１は、プログラムメモリ１２に記録されたプログラムに従いデータメモリ１３を使用して内部処理を行なう。データメモリ１３には、アプリケーション毎、ＥＦ（Elementary File）が割り付けられ、ＤＦ（Directory File）で示されるアプリケーションを格納する領域に対し、例えば、キャッシュカード取引、デビットカード取引を行なうための複数種の取引データが格納される。本発明と関係するところでは、どの秘密鍵を利用した証明書かを特定するためのインデックスと関連付けられた公開鍵が格納される領域Ａの他に、ＣＡ公開鍵を用いて証明書が検証された公開鍵を保存するためのテンポラリ領域Ｂが割り付けられている。

【００１５】図２は、本発明に従う鍵管理の一例を表形式で示した図である。図２において、各発行者の公開鍵および秘密鍵に付与されている番号がその対応関係を示している。図中、証＜秘１＞とは、ＣＡ秘密鍵１を用いて生成された公開鍵証明書を表し、”公１”とは公開鍵１を表す。なお、図２では、秘密鍵の有効期間によってフェーズを区分しており、ＣＡでの鍵管理、金融機関（発行者）での鍵管理、ＩＣカード１０へ格納する発行者証明書および鍵、ＡＴＭ端末３０へ格納する端末公開鍵証明書および鍵のそれぞれの鍵更新スケジュールが示されている。ＩＣカード１０および端末の欄に記載されている矢印は、その期間において、証明書および公開鍵を新規に作成、または更新する場合にはどのような内容になるかを示す。例えば、サービス開始時において、新規のカードを発行する場合には、証明書＜秘1or2＞、ならびに公開鍵１および公開鍵２を設定することになる。

【００１６】ところで、ＩＣカード１０とＡＴＭ端末３０において保持している証明書、公開鍵が異なる場合がある。その場合は、上記したように、証明書作成に用いた秘密鍵と対応する公開鍵が公開鍵インデックとして指定されているため、その指定された公開鍵を用いて認証処理を行なう。すなわち、ＩＣカード１０内には、ＣＡ公開鍵とそのＣＡのインデックスとを組み合わせて複数格納されている。そして、ＩＣカード１０内で外部ノードの公開鍵証明書を検証する場合、その外部ノードでは、公開鍵証明書と共にその証明書を付与したＣＡのインデックスと共にＩＣカード１０内に送信する。ＩＣカード１０では、内部で格納されたＣＡのインデックスと送信されたＣＡのインデックスとを比較照合して、等しいものが見つかったときにそれに関連付けられたＣＡの公開鍵で検証する。このインデックスにより現在有効となっている公開鍵が特定できる。

【００１７】図３に、ＩＣカード１０、ＡＴＭ端末３０のそれぞれにおけるＣＡ公開鍵および証明書の格納形態が、それぞれ、（ａ）、（ｂ）で示され、また、図４に証明書検証処理の動作概念が示されている。図３に示されるように、証明書鍵発行者であるＣＡの鍵の更新時に

おいてその運用やサービスを制限することなく、当該鍵を更新することに対応するため、ＩＣカード１０内部には、２組のＣＡ公開鍵とＣＡ公開鍵インデックス（ＩＣカード検証用）、１組の発行者公開鍵証明書、ＩＣカード公開鍵証明書とＣＡ公開鍵インデックス（ＩＣカード・証明書）を持つ。カード１０内部への関連データの格納形態は図示したとおりである。ここでは、ＲＳＡ暗号化の例が示されている。証明書データは、対応するＣＡ公開鍵に付与されているＣＡインデックス（ＩＣカード・証明書）と関係付けられる。

【００１８】外部から証明書データを受信すると種々のチェックを実行後、ディジタル署名の検証が行なわれる。この検証は、ＩＣカード１０内部における２つのＣＡ公開鍵の組のうち、端末公開鍵証明書とＣＡ公開鍵インデックス（ＩＣカード・検証用）が等しい組のＣＡ公開鍵を利用する。この様子は図４に示されている。どちらのＣＡ公開鍵インデックス（ＩＣカード・検証用）とも異なる場合、および正常に終了しなかった場合はコマンド処理を中断する。

【００１９】図５は、カード認証の流れを説明するために引用した図であり、具体的には、図６に示される「ＣＡ－発行者（金融機関）－ＩＣカード」から成る階層化された公開鍵管理体系における、証明書検証ならびに公開鍵抽出シーケンスが示されている。ここでは、上記した公開鍵管理体系の中で、ＩＣカード１０とＡＴＭ端末３０間の動作シーケンスのみ抽出して示している。

【００２０】動作説明に先立ち、カード発行者である金融機関は、ＣＡに自身の公開鍵を登録し、当該鍵に対する証明書を発行してもらう。また、金融機関は、自らが発行する各ＩＣカード１０に対する公開鍵、秘密鍵のペアを作成し、自身の秘密鍵によって証明書を生成する。更に、ＡＴＭ端末３０においては、個々の端末に対する公開鍵、秘密鍵のペアを作成し、ＣＡにより生成された証明書をＡＴＭ端末３０に格納してあるものとする。

【００２１】上記した前提の下、まず、ＡＴＭ端末３０は、ＩＣカード１０から発行者公開鍵証明書、ＣＡ公開鍵およびその世代番号が示されるインデックス他の情報を読み出す（ステップＳ３１），これら情報を得たＡＴＭ端末３０は、内部でSET PUBLIC IC KEYコマンドを発行し、第１階層、ここでは発行者公開鍵証明書の検証を行なう（ステップＳ３２）。SET PUBLIC IC KEYコマンドは、外部ノードから送られる公開鍵の証明書をＩＣカード１０内に格納されている公開鍵またはテンポラリ公開鍵を用いて検証し、当該公開鍵をＡＴＭ端末３０内に設定するために使用されるコマンドであり、本コマンドで設定した公開鍵は、再度本コマンドを使用して設定するまで、または、設定した公開鍵を用いた認証コマンドが実行されるまで有効とするものである。

【００２２】特徴的には、このSET PUBLIC IC KEYコマンドには、ＩＣカード１０の証明書を検証するコマンドにＣＡ公開鍵を用いて検証するインタフェースが備えられていることである。ここで得られるＣＡ公開鍵を用いて証明書が検証された公開鍵は「テンポラリ公開鍵」としてＩＣカード１０内の一時記憶領域Ｂに保存される（ステップＳ３３）。直後、SET-PUBLIC-IC-KEYコマンドにより、上記により設定された「テンポラリ公開鍵」を指定してＩＣカード公開鍵証明書の内部にある公開鍵を抽出して第２階層、ここでは、ＩＣカード公開鍵証明書の検証を行ない（ステップＳ３４、Ｓ３５）、テンポラリ公開鍵を保存する（ステップＳ３６）。

【００２３】更に、キャッシュカードやデビットカードによる取引があったとき（ステップＳ３７）、先に設定された公開鍵に基づき、認証コマンド（EXTERNAL AUTHENTICATE）を用いて外部認証（暗号化されたデータ内容のチェック）を行なう（ステップＳ３８）。なお、テンポラリ公開鍵が設定されていて、テンポラリ公開鍵を用いた外部認証に失敗した場合は（ステップＳ４１）、テンポラリ公開鍵を設定する際、最初に利用した鍵（ＡＴＭ端末３０に記録されているＣＡ公開鍵）の再試行回数がカウントアップされ（ステップＳ４２）、成功した場合はクリアされる（ステップＳ４３）。また、再試行回数がＡＴＭ端末３０に設定されている最大許容再試行回数を超えた場合にはＣＡ公開鍵がロックされる（ステップＳ４４、Ｓ４５）。再試行回数および最大許容再試行回数はＣＡ公開鍵に関連付けられているものとする。

【００２４】以上説明のように、ＣＡ公開鍵を用いて証明書が検証された公開鍵はテンポラリ公開鍵としてＡＴＭ端末３０内に保存され、ＩＣカード１０の証明書を検証するコマンドを用いてそのテンポラリ公開鍵を指定し、当該テンポラリ公開鍵を用いて次階層の証明書を検証し、証明書が検証された公開鍵はテンポラリ公開鍵として保存される。そして、外部認証時、そのテンポラリ公開鍵を用いた検証を行なうことで取引が実行される。このように、テンポラリ公開鍵の利用により複数階層の検証が大量の証明書データの送信なくして可能となる。なお、上記した実施形態では、ＡＴＭ端末３０が階層化された証明書検証および公開鍵抽出を行なうものとして説明したが、ＩＣカード１０に置換えても同様に実行可能である。

【００２５】

【発明の効果】以上説明のように本発明によれば、ＩＣカード内にＣＡ公開鍵とそのＣＡのインデックスを組み合わせて複数格納し、ＩＣカードで外部ノードの公開鍵証明書を検証するとき、公開鍵証明書と共にその証明書を付与したＣＡのインデックスをＩＣカード内に送信し、ＩＣカードでは、その格納されたＣＡのインデックスと送信されるＣＡのインデックスとを照合し、関連付けられたＣＡ公開鍵で検証することにより、複数種類の秘密鍵による証明書が出回ってもＩＣカードでの検証を可能とし、セキュリティを維持しつつ信頼性及び処理速

度の向上を図ることができる。

【００２６】また、ＣＡ公開鍵を用いて証明書が検証された公開鍵はテンポラリ公開鍵としてＩＣカード内に保存され、ＩＣカードの証明書を検証するコマンドを用いてそのテンポラリ公開鍵を指定し、当該テンポラリ公開鍵を用いて次階層の証明書を検証し、証明書が検証された公開鍵はテンポラリ公開鍵として保存される。このことにより、複数階層の証明書の検証を実現でき、外部認証時、そのテンポラリ公開鍵を用いた検証を行なうことで、ＩＣカードの記憶容量の節約ができ、また、汎用的なコマンドを複数回実行することで、証明書の検証ならびに公開鍵の抽出を実現できるため、検証のためのＩＣカードのプログラム容量の削減、拡張性の改善が図られる。

【図面の簡単な説明】

【図１】　本発明において使用されるＩＣカードの内部構成を示すブロック図である。

【図２】　本発明のディジタル署名システムによる鍵管理の一例を表形式で示した図である。

【図３】　ＩＣカード、ＡＴＭのそれぞれにおけるＣＡ公開鍵および証明書の格納形態を説明するために引用した図である。

【図４】　本発明実施形態の動作を説明するために引用した図であり、証明書検証処理の動作概念図である。

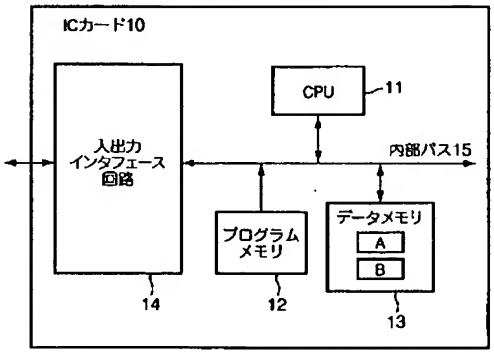
【図５】　本発明のディジタル署名システムの動作をシーケンスチャートで示した図である。

【図６】　本発明の前提となる証明書発行体系を説明するために引用した図である。

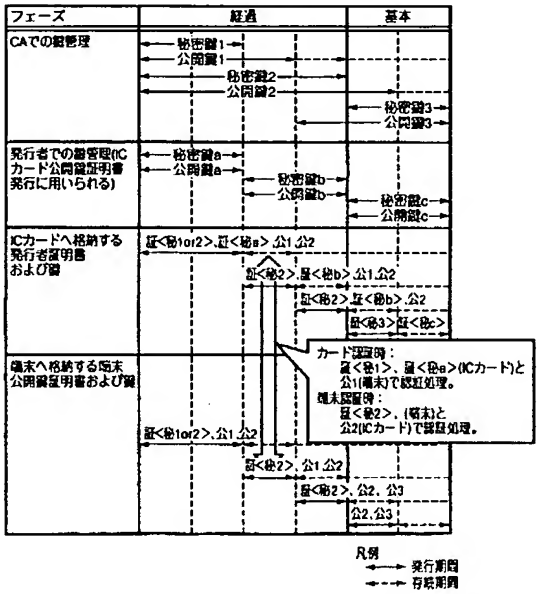
【符号の説明】

１０…ＩＣカード、１１…ＣＰＵ、１２…プログラムメモリ、１３…データメモリ、１４…入出力インタフェース回路１５…内部バス、３０…ＡＴＭ端末

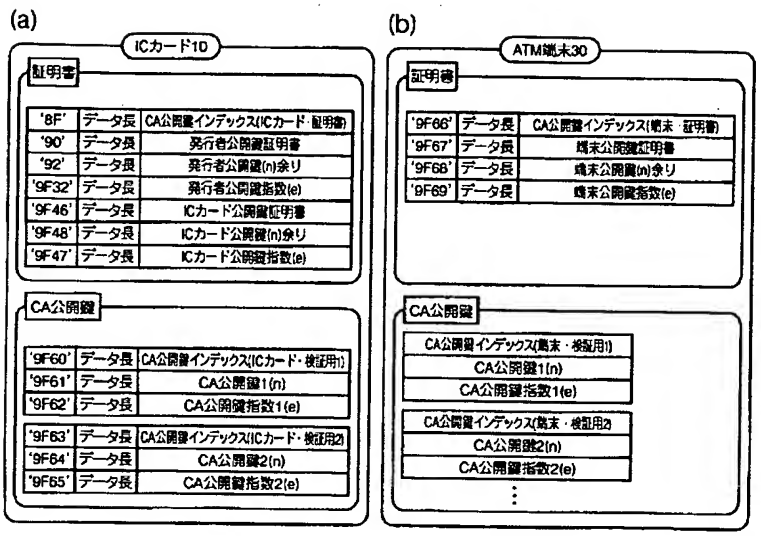
【図１】



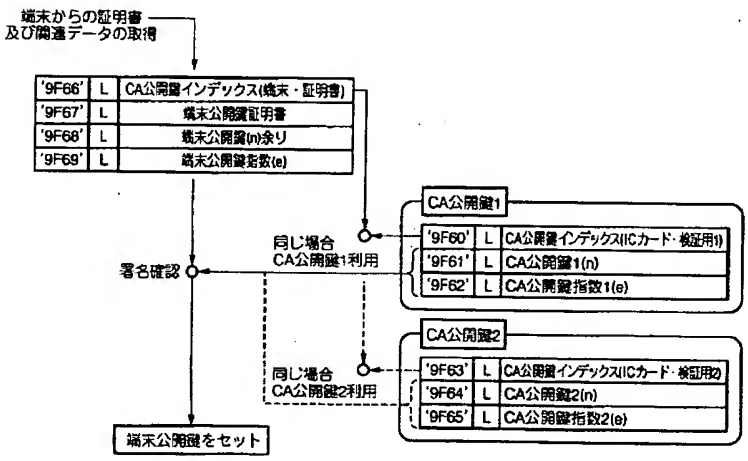
【図２】



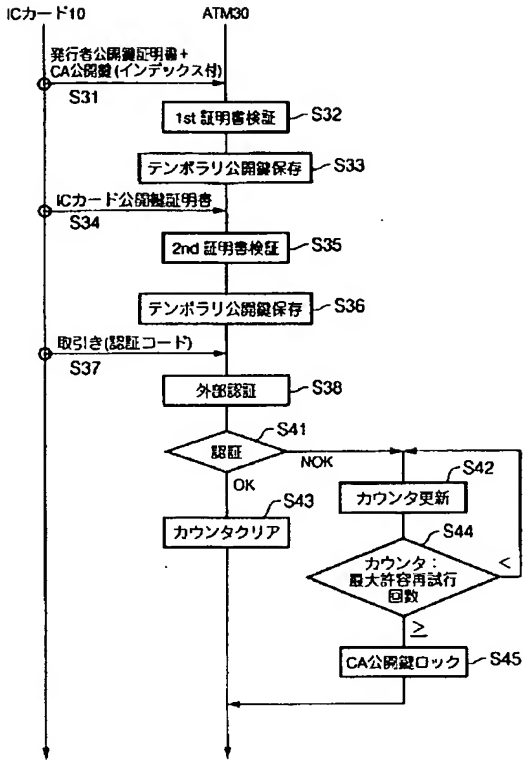
【図3】


(a)
ICカード10
証明書
'8F' データ長 CA公開鍵インデックス(ICカード・証明書)
'90' データ長 発行者公開鍵証明書
'92' データ長 発行者公開鍵(n)余り
'9F32' データ長 発行者公開鍵指数(e)
'9F46' データ長 ICカード公開鍵証明書
'9F48' データ長 ICカード公開鍵(n)余り
'9F47' データ長 ICカード公開鍵指数(e)
CA公開鍵
'9F60' データ長 CA公開鍵インデックス(ICカード・検証用1)
'9F61' データ長 CA公開鍵1(n)
'9F62' データ長 CA公開鍵指数1(e)
'9F63' データ長 CA公開鍵インデックス(ICカード・検証用2)
'9F64' データ長 CA公開鍵2(n)
'9F65' データ長 CA公開鍵指数2(e)
(b)
ATM端末30
証明書
'9F66' データ長 CA公開鍵インデックス(端末・証明書)
'9F67' データ長 端末公開鍵証明書
'9F68' データ長 端末公開鍵(n)余り
'9F69' データ長 端末公開鍵指数(e)
CA公開鍵
CA公開鍵インデックス(端末・検証用1)
CA公開鍵1(n)
CA公開鍵指数1(e)
CA公開鍵インデックス(端末・検証用2)
CA公開鍵2(n)
CA公開鍵指数2(e)

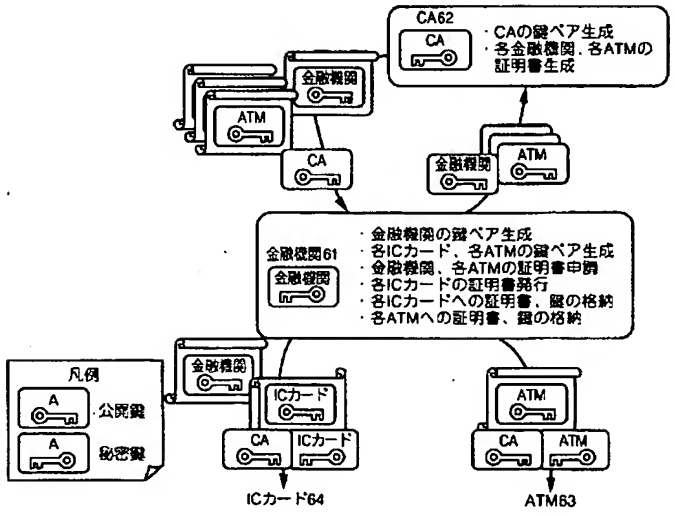
【図4】


端末からの証明書及び関連データの取得
'9F66' L CA公開鍵インデックス(端末・証明書)
'9F67' L 端末公開鍵証明書
'9F68' L 端末公開鍵(n)余り
'9F69' L 端末公開鍵指数(e)
署名確認
同じ場合 CA公開鍵1利用
同じ場合 CA公開鍵2利用
CA公開鍵1
'9F60' L CA公開鍵インデックス(ICカード・検証用1)
'9F61' L CA公開鍵1(n)
'9F62' L CA公開鍵指数1(e)
CA公開鍵2
'9F63' L CA公開鍵インデックス(ICカード・検証用2)
'9F64' L CA公開鍵2(n)
'9F65' L CA公開鍵指数2(e)
端末公開鍵をセット

【図5】


ICカード10
ATM30
発行者公開鍵証明書+
CA公開鍵(インデックス付)
S31
1st 証明書検証
S32
テンポラリ公開鍵保存
S33
ICカード公開鍵証明書
S34
2nd 証明書検証
S35
テンポラリ公開鍵保存
S36
取引き(認証コード)
S37
外部認証
S38
認証
S41
NOK
OK
S42
カウンタ更新
S43
カウンタクリア
S44
カウンタ:
最大許容再試行
回数
<
≧
CA公開鍵ロック
S45

【図6】


CA62
CA
・CAの鍵ペア生成
・各金融機関、各ATMの
証明書生成
金融機関
ATM
CA
金融機関
ATM
金融機関61
金融機関
・金融機関の鍵ペア生成
・各ICカード、各ATMの鍵ペア生成
・金融機関、各ATMの証明書申請
・各ICカードの証明書発行
・各ICカードへの証明書、鍵の格納
・各ATMへの証明書、鍵の格納
凡例
A
公開鍵
A
秘密鍵
金融機関
ICカード
CA
ICカード
ICカード64
ATM
CA
ATM
ATM63

フロントページの続き

(72)発明者　星川　知之
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(72)発明者　岩瀬　史幸
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(72)発明者　三輪　哲也
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(72)発明者　増田　豊
東京都千代田区丸ノ内一丁目３番１号　社団法人東京銀行協会内
(72)発明者　前田　亮
東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内
(72)発明者　奥平　進
東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内